Chapter 2: Principals, Accounts and Passwords

Virtually all computers on-site are required to run Kerberos authentication. You'll need to get a *Kerberos principal* (a special userid which identifies you to the Kerberos authentication system) plus an initial Kerberos password. On any computer you plan to use, you still need to have an account created for yourself, with an initial password. You'll need to change your initial passwords. In this chapter you'll find out how to do these things.

2.1 Choose and Obtain a Kerberos Principal and Password

2.1.1 Kerberos Principal

We recommend that you obtain a Kerberos principal and password before creating or requesting any computer accounts.

See **Strong Authentication at Fermilab** section *4.1 Your Kerberos Principal* at `http://www.fnal.gov/docs/strongauth/html/princ_pw.html#33181`). Request a principal using the online form **Request Form for Computing Username and Primary Accounts** at `http://www.fnal.gov/cd/forms/acctreq_form.html`. From this form you can request other items you may need as well.

If you will require access from a nonKerberized machine or from any X terminal, request a CRYPTOCard when you request your principal. CRYPTOCards are discussed in section 3.5 *Connecting from a NonKerberized Machine to Kerberized Host* and in **Strong Authentication at Fermilab** section 5.5 *Connecting from a NonKerberized Machine: Portal Mode*.

2.1.2 Kerberos Password

Once your request for a principal has been approved, you must stop by WH8NE (Yolanda Valadez' office) to receive your initial Kerberos password. If you are off-site, you can get it over the telephone (630-840-8118). You cannot get it via email.

You are required to change the initial password within 30 days of its creation, and roughly once a year thereafter. Refer to **Strong Authentication at Fermilab** section 2.4.1 *Your Kerberos Password* for instructions.

In contrast to the principal (which ideally should match your login name on each machine and your email address), we ask that your Kerberos password be unique. That is, in order to avoid exposing your Kerberos password, it must be different from the passwords you use for any other purpose. We ask also that you treat your password as a sacred object; please refer to the guidelines listed on the page `http://computing.fnal.gov/orientation/policy.html`.

The Fermilab Computer Security Team has imposed some restrictions on passwords in accordance with DOE guidelines. Passwords the system considers "bad" will be rejected.

For information about passwords, see **Strong Authentication at Fermilab** section *4.2 Your Kerberos Password* (`http://www.fnal.gov/docs/strongauth/html/princ_pw.html#46115`).

2.2 Obtain a Computer Account

To request an FNALU account, use the **Request Form for Computing Username and Primary Accounts** online at `http://www.fnal.gov/cd/forms/acctreq_form.html`. For accounts on other UNIX systems, consult the system administrators of those systems.

We strongly recommend that you use your principal name as your login id (account name) on all Fermilab computer systems. There are significant conveniences if your principal and your account name are the same, as discussed in **Strong Authentication at Fermilab** *Appendix C. More about Choosing a Principal Name*.

Maybe it's more effective to say that there are *significant disadvantages* to choosing a login id that does *not* match your principal!

A UNIX login id must consist of lower case characters only. Be sure to enter them in the correct case, because UNIX is case-sensitive. Note that if you do accidentally use upper case to log in, UNIX may assume you have an upper-case-only terminal and you will have very limited capability. In this case, either log out and log back in again, or enter the command:

```
% stty -lcase
```

When you get an account on a machine, you will also get an initial password. Read the following section, then change the password using the instructions in section 2.4 *Changing Passwords*.

2.3 Other Passwords

2.3.1 The Standard UNIX Password

There exist passwords other than your Kerberos password that can be enabled for your account on UNIX systems: a local UNIX password, an AFS password[1], and an NIS password. Unlike the Kerberos password, these passwords do not authenticate you to Kerberized services, and consequently they disallow single sign-on access to other systems.

We may turn off the NIS passwords for each on-site system as it becomes Kerberized; in any case they will no longer be useful or necessary.

If you log in with one of these passwords directly to the console of a computer, you may run the Kerberos command **`kinit`**, provide your Kerberos password as prompted, and obtain Kerberos credentials. Your credentials allow you to access other Kerberized systems with no further authentication required.

2.3.2 The Standard UNIX Password

You generally have a standard UNIX password on all UNIX computers, whether or not they're strengthened (if AFS is installed, you have an AFS password either in addition to or instead of a UNIX password).

1. In previous editions of this document, an AFS password was frequently called a "Kerberos password". This referred to Kerberos V4 which is integrated into AFS. In the current edition of this document, "Kerberos password" always refers to Kerberos V5, the product we use to implement strong authentication, and when discussing Kerberos V4 or AFS, we specify "AFS", e.g., "AFS password".

A UNIX password can be used to log in at the console of a strengthened machine, thus allowing you to log into it even if you cannot be authenticated via Kerberos for one reason or another, or if there's no Kerberized local login[1]. No access to Kerberized services (e.g., Kerberized telnet, ssh) is granted until you manually run the **`kinit`** command.

A UNIX password can be used to log in at the console of a machine running AFS, but you will not be granted access to the file system or to Kerberized services until you run the **`kinit`** command.

As long as the Fermilab Kerberos authentication system is up and running, you should never need to use, change, or be concerned about your UNIX password.

2.3.3 The AFS Password

AFS, described in Chapter 8: *The AFS File System* is installed on many UNIX systems at Fermilab. AFS may be installed on a given system such that you have only an AFS password, and no standard UNIX password is defined (this is the case on FNALU). You can find out if you have a standard UNIX password by attempting to change it via the standard UNIX command **`passwd`**. If the command does not succeed (assuming you provide the correct old password as requested), then you do not have a standard UNIX password.

There are three common situations in which your AFS password is useful and/or necessary:

1) When logging into strengthened UNIX systems running AFS, your AFS password would be useful to log in to the console and get access to the file system but not to Kerberized services.

2) To get/renew an AFS token on a remote system, you'd need to enter your AFS password if your local system doesn't run AFS (see section 8.3.1 *Authentication in AFS*). (When you authenticate to Kerberos on your local machine, you don't get an AFS token if AFS isn't running, so you have none to forward).

3) If you ever need to manipulate files and directories in AFS space from a Windows machine, you can install the Windows AFS client on that machine. The Windows AFS client allows you to map directories under Fermilab's AFS cell to your Windows machine so that these directories appear as mounted drives, just as local or networked Windows resources do. You can then move and copy files to and from AFS drives/folders the same as you do between your other drives/folders. Authentication using your AFS password is sufficient; you do not authenticate via Kerberos to the FNAL.GOV realm in this case.

---

1. Kerberized local login for IRIX systems or GUI login is available via vendor-supplied PAMs.

2.3.4 UNIX and AFS Password Recommendations

Choose your UNIX and/or AFS password(s) to be different from your Kerberos password! Otherwise you risk exposing your Kerberos password and compromising the security.

A standard UNIX password must be at least six characters long and should not be your login name or any simple permutation of it. We recommend that you limit your password to eight characters, especially if it is used as an AFS password. It is advisable to mix letters and digits in your password.

2.4 Changing Passwords

2.4.1 Your Kerberos Password

Please read the information and instructions in the **Strong Authentication at Fermilab** document, section *3.3 Changing your Kerberos Password* and section *3.3.1 UNIX/Linux/Cygwin*.

If you've already read the information and you just need to remember the command, here it is. Log in locally to your desktop or laptop and run:

```
% kpasswd [<principal-name>]
```

Make sure this runs `/usr/krb5/bin/kpasswd`.

If the password has expired, you'll need to log in using your standard UNIX password, then run **`kpasswd`**.

2.4.2 Your UNIX Password

A UNIX password is stored, and thus may be changed, in one of two ways, depending on the configuration of your system:

- If your system uses the standard UNIX file system, and NIS is not installed, your UNIX password is part of your local password file, and can be changed via the **`passwd`** command. Your UNIX password is only changed for the machine, or node, on which you execute this command.

- If NIS[1] is running on your system, your UNIX password is stored in the NIS password file[2] which is shared by all machines on the NIS cluster, and can be changed via the **`yppasswd`** command. In this case your UNIX password is changed for all nodes of the NIS cluster.

For any password changes, you will be prompted for your old and new passwords.

2.4.3 Your AFS Password

You can change your AFS password via the command **`kpasswd`** (**`/usr/afsws/bin/kpasswd`**). (Note that **`kpasswd`** is used to change the Kerberos password as well, as discussed in section 2.4.1 *Your Kerberos Password*, and on strengthened systems its path should precede the AFS **`kpasswd`** path in the $PATH variable.) You will be prompted for your old and new passwords. This changes your AFS password for all the AFS nodes at Fermilab.

1. NIS (Network Information System) is a distributed database used to manage a network of computers.
2. The passwords in the NIS maps have been turned off .